Impact model-driven software verification on software testing

verum®

Tools for building mathematically verified software

ASD in practice

Leon Bouwmeester, development manager Verum

Agenda

verum

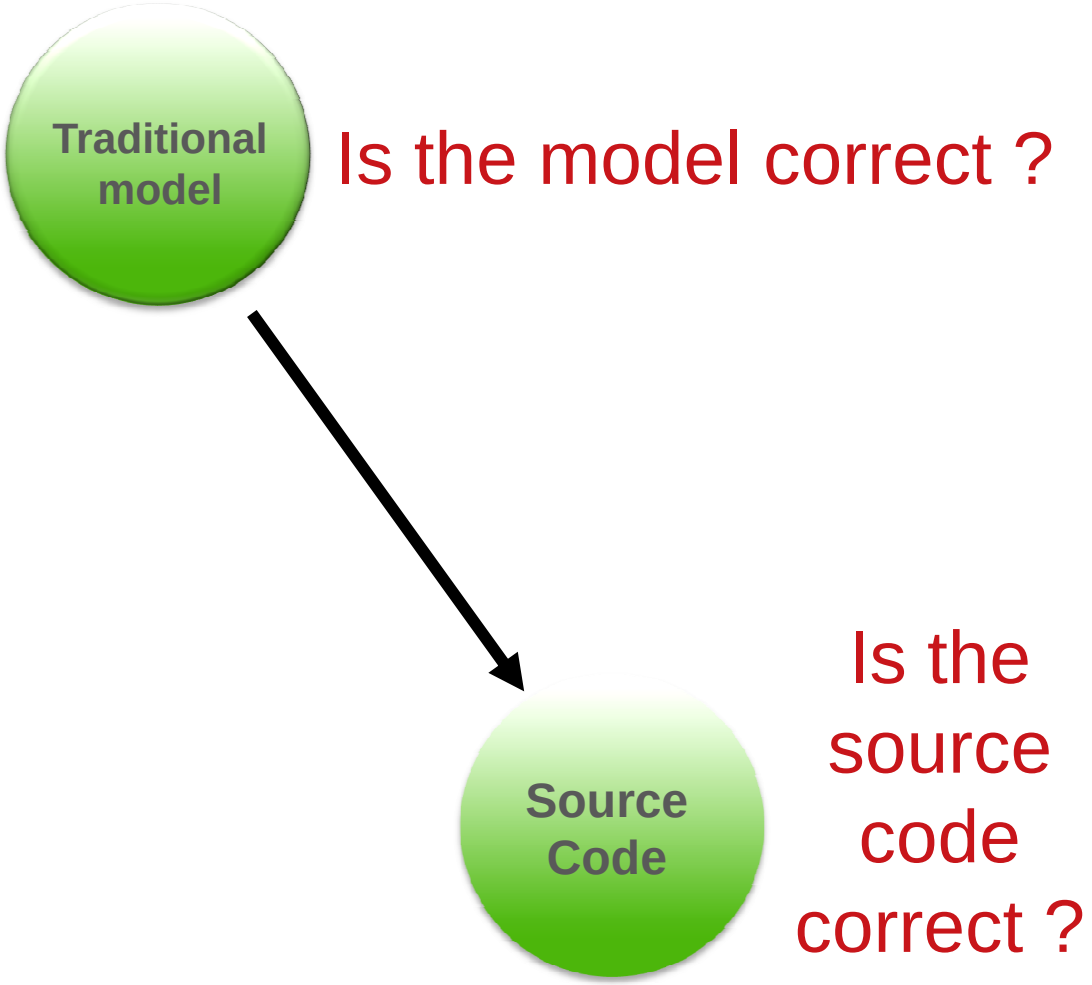
- ASD: what is it and how does it work?
- Impact of ASD on development process
  - On system testing in particular
- Future extensions of ASD
  - Impact on system testing

What is ASD?

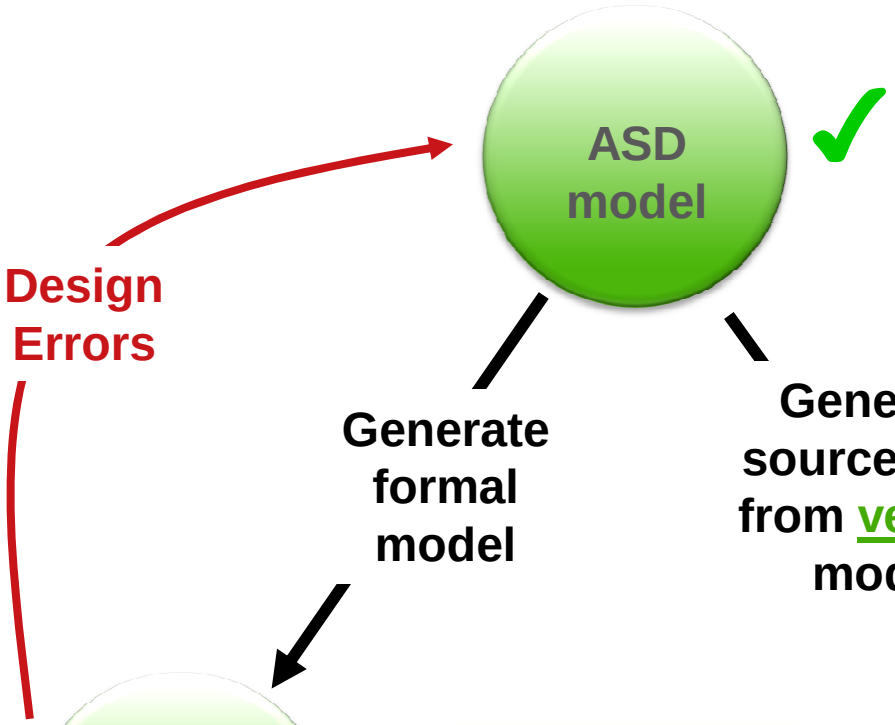
verum

- Analytical Software Design
- ASD is a component-based technology supported by a toolset for:
  - constructing correct industrial scale systems from verified components
- ASD provides:
  - Support for specification of interface and design models
  - Visual verification based on automatic generation of formal models
  - Automatic code generation (Java, C++, C#, MISRA-C)
- ASD guarantees:
  - equivalence between ASD models, formal models and runtime behaviour of generated code

Why is it different



Why is it different



- **ASD Models are:**
  - **Precise**
  - **Complete**
  - **Traceable**
  - **Correct**

- **MISRA C**
- **C++**
- **C#**
- **Java**

EU patent 1749264

Hong Kong patent HK 1104100

Semiconductor industry case

verum

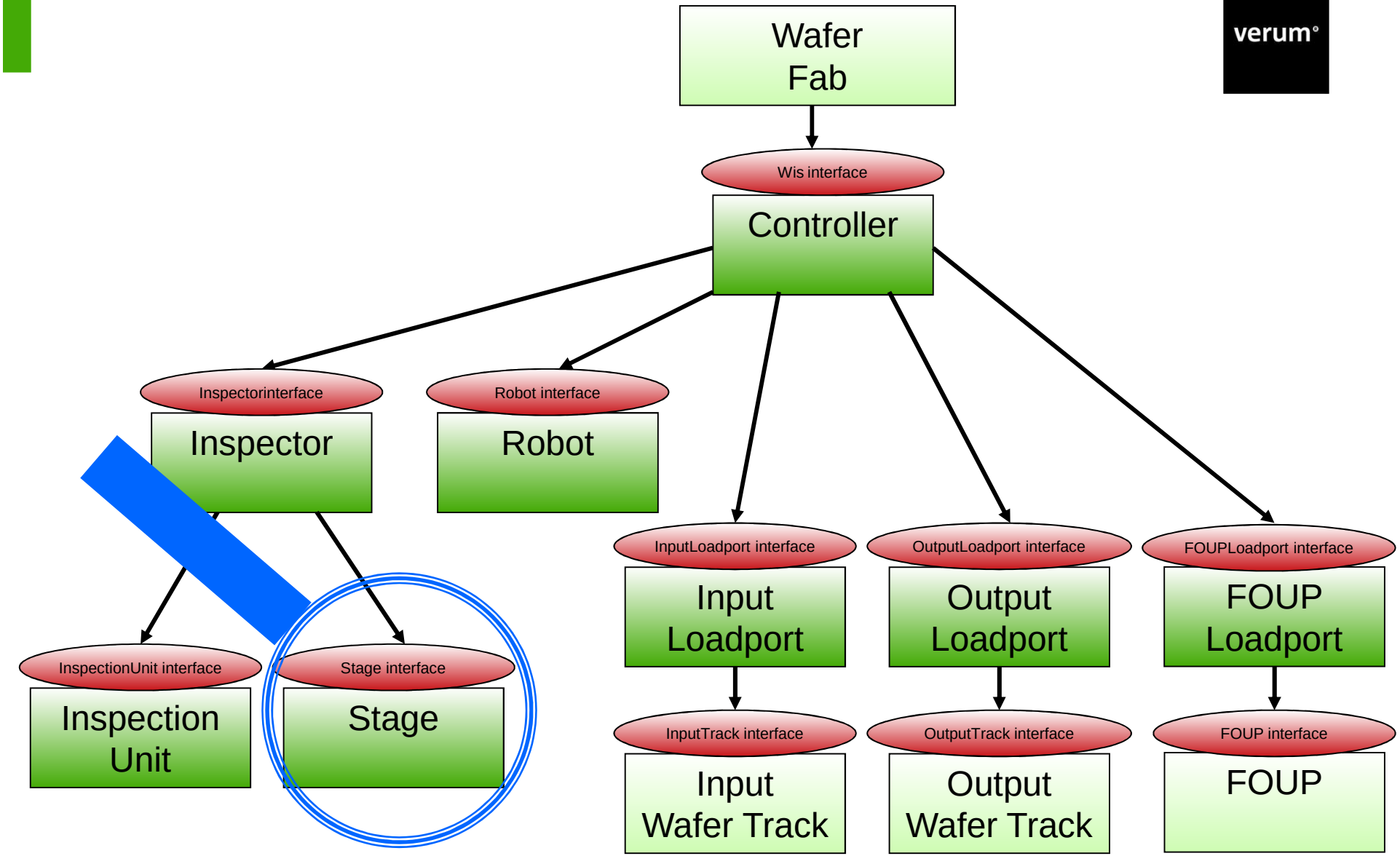
- **Nanda Technologies GmbH** builds wafer inspection systems
  - Robot, lamps, camera, filters, sensors, safety shutters, ..
  - Lot of signals to process
    - External wafer control requests
    - Hardware feedback (functional and failures)
    - Parallelism needed for optimal throughput
  - Lack of time and people

Nanda | Tech

- Nanda Tech decided to use Verum's ASD technology

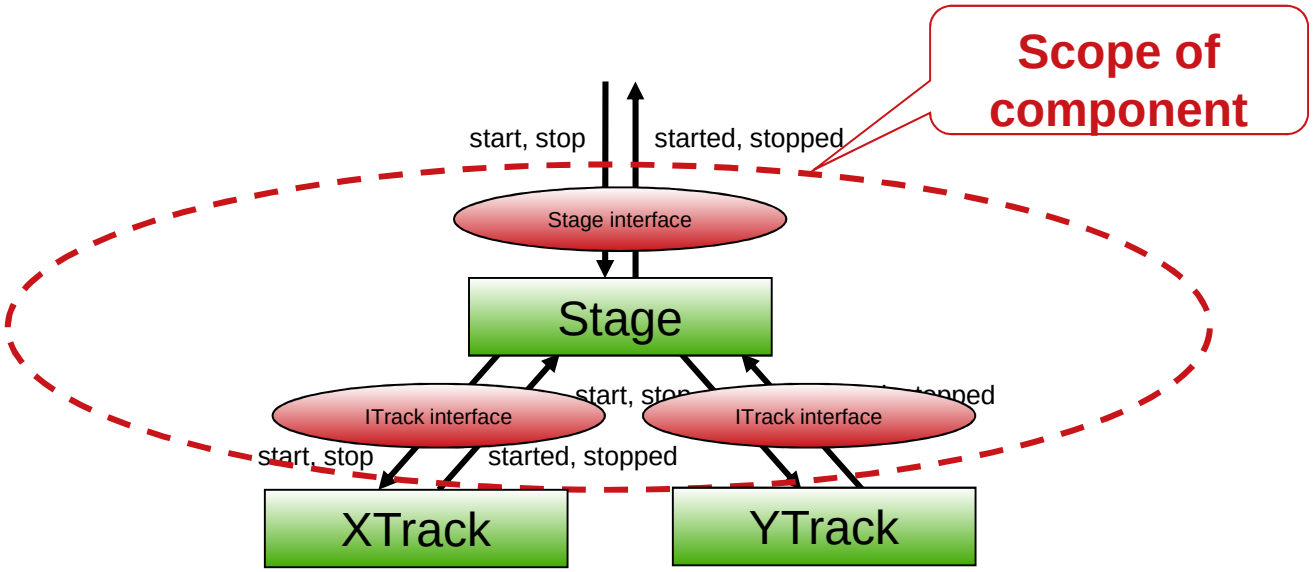
Software architecture (simplified)

verum



Stage Design

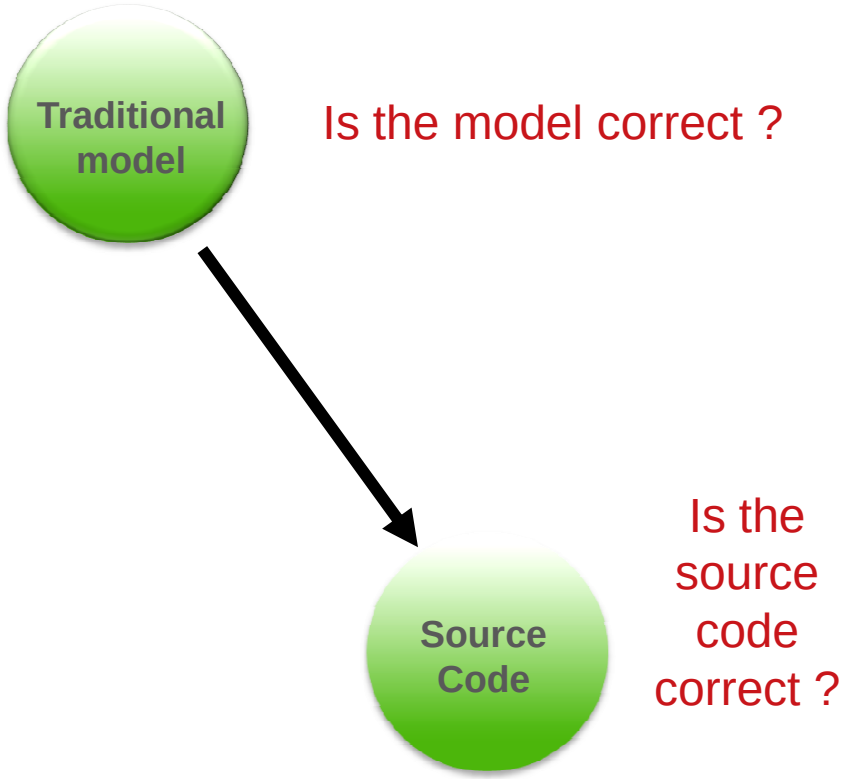
verum



First attempt

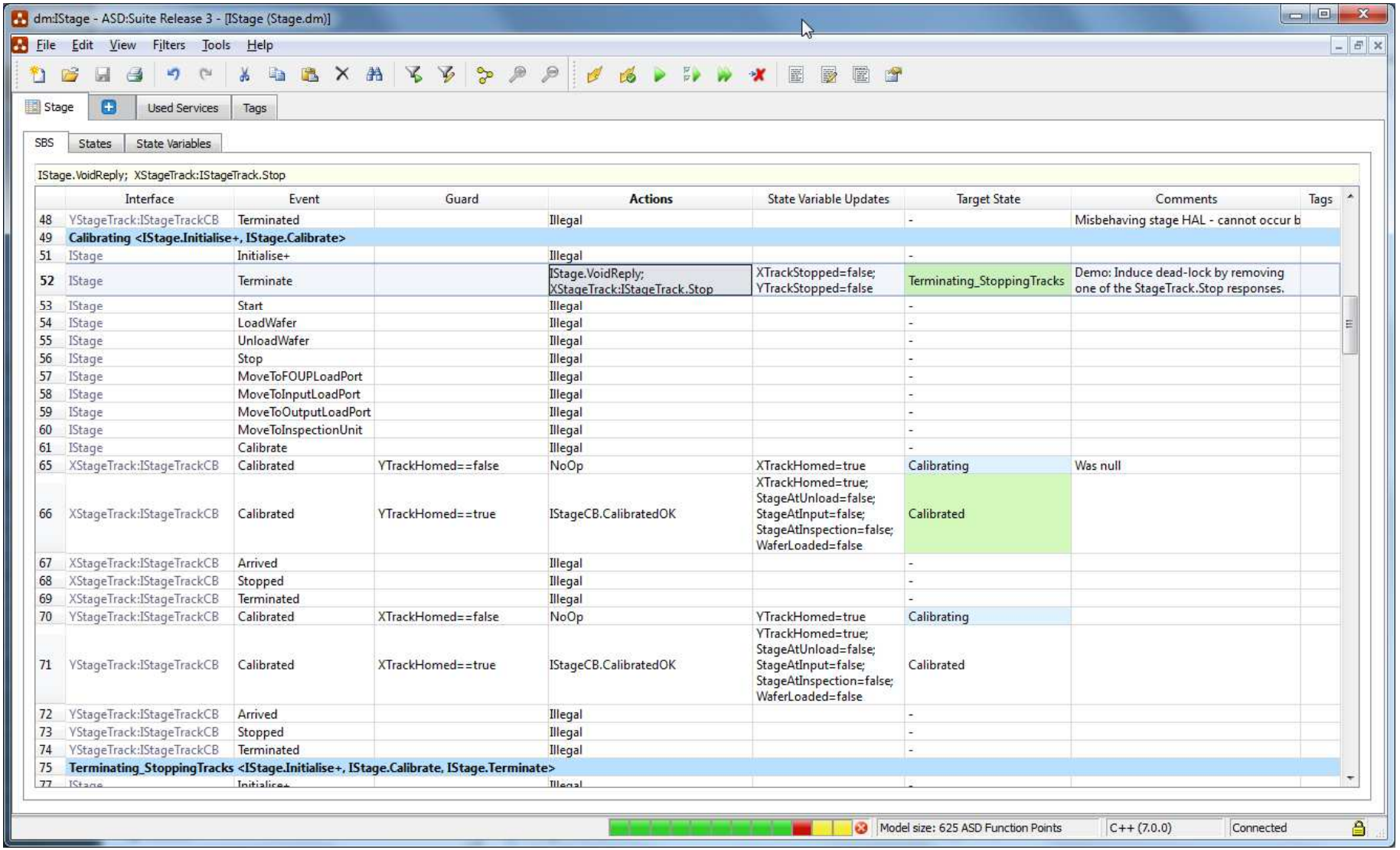
verum

- Make models
- Use code generator to automatically generate code (not verified)



First attempt: design model

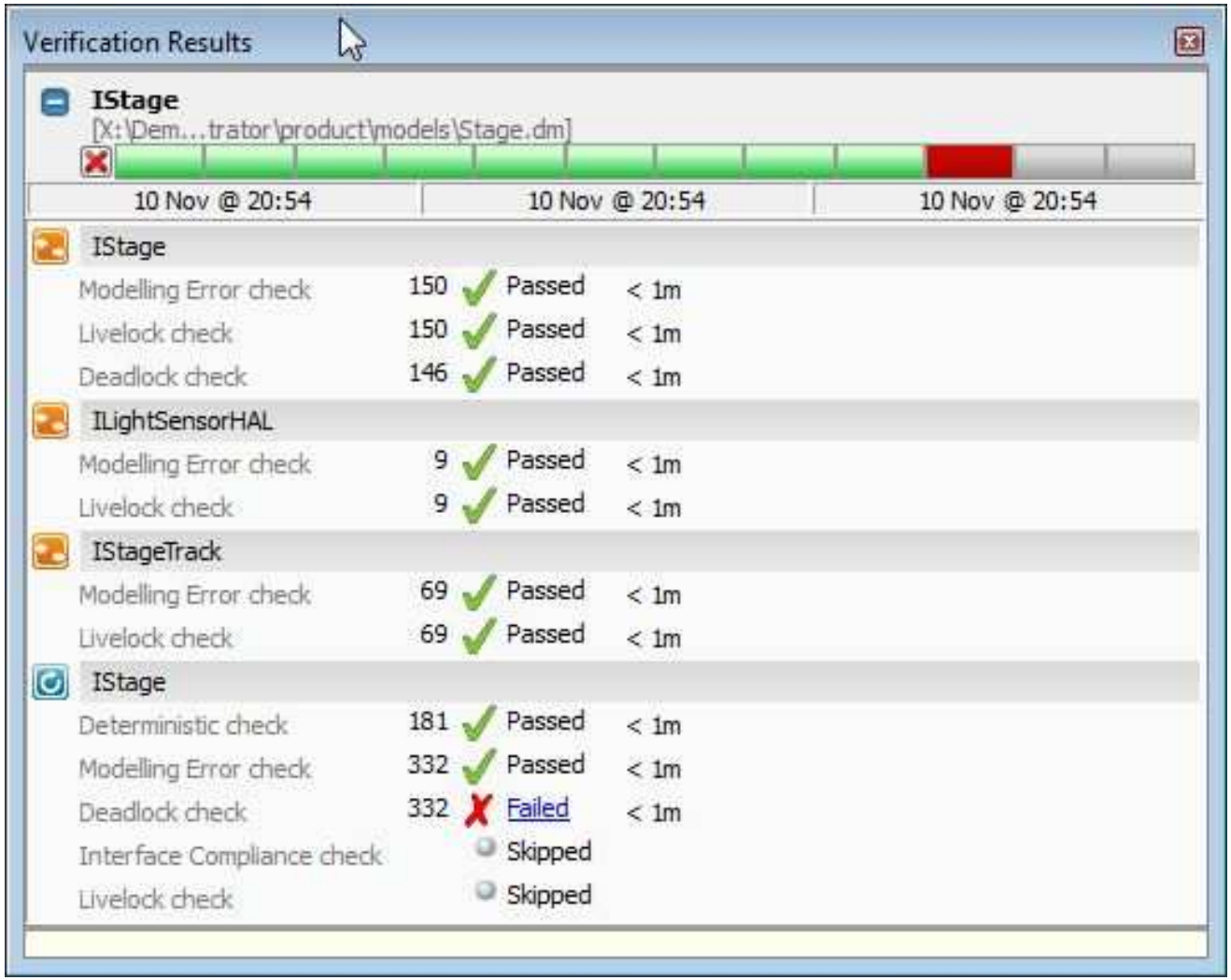
verum



	Interface	Event	Guard	Actions	State Variable Updates	Target State	Comments	Tags
48	YStageTrack:IStageTrackCB	Terminated		Illegal		-	Misbehaving stage HAL - cannot occur b	
49	**Calibrating <IStage.Initialise+, IStage.Calibrate>**							
51	IStage	Initialise+		Illegal		-		
52	IStage	Terminate		IStage.VoidReply; XStageTrack:IStageTrack.Stop	XTrackStopped=false; YTrackStopped=false	Terminating_StoppingTracks	Demo: Induce dead-lock by removing one of the StageTrack.Stop responses.	
53	IStage	Start		Illegal		-		
54	IStage	LoadWafer		Illegal		-		
55	IStage	UnloadWafer		Illegal		-		
56	IStage	Stop		Illegal		-		
57	IStage	MoveToFOUPLoadPort		Illegal		-		
58	IStage	MoveToInputLoadPort		Illegal		-		
59	IStage	MoveToOutputLoadPort		Illegal		-		
60	IStage	MoveToInspectionUnit		Illegal		-		
61	IStage	Calibrate		Illegal		-		
65	XStageTrack:IStageTrackCB	Calibrated	YTrackHomed==false	NoOp	XTrackHomed=true	Calibrating	Was null	
66	XStageTrack:IStageTrackCB	Calibrated	YTrackHomed==true	IStageCB.CalibratedOK	XTrackHomed=true; StageAtUnload=false; StageAtInput=false; StageAtInspection=false; WaferLoaded=false	Calibrated		
67	XStageTrack:IStageTrackCB	Arrived		Illegal		-		
68	XStageTrack:IStageTrackCB	Stopped		Illegal		-		
69	XStageTrack:IStageTrackCB	Terminated		Illegal		-		
70	YStageTrack:IStageTrackCB	Calibrated	XTrackHomed==false	NoOp	YTrackHomed=true	Calibrating		
71	YStageTrack:IStageTrackCB	Calibrated	XTrackHomed==true	IStageCB.CalibratedOK	YTrackHomed=true; StageAtUnload=false; StageAtInput=false; StageAtInspection=false; WaferLoaded=false	Calibrated		
72	YStageTrack:IStageTrackCB	Arrived		Illegal		-		
73	YStageTrack:IStageTrackCB	Stopped		Illegal		-		
74	YStageTrack:IStageTrackCB	Terminated		Illegal		-		
75	**Terminating_StoppingTracks <IStage.Initialise+, IStage.Calibrate, IStage.Terminate>**							
77	IStage	Initialise+		Illegal		-		

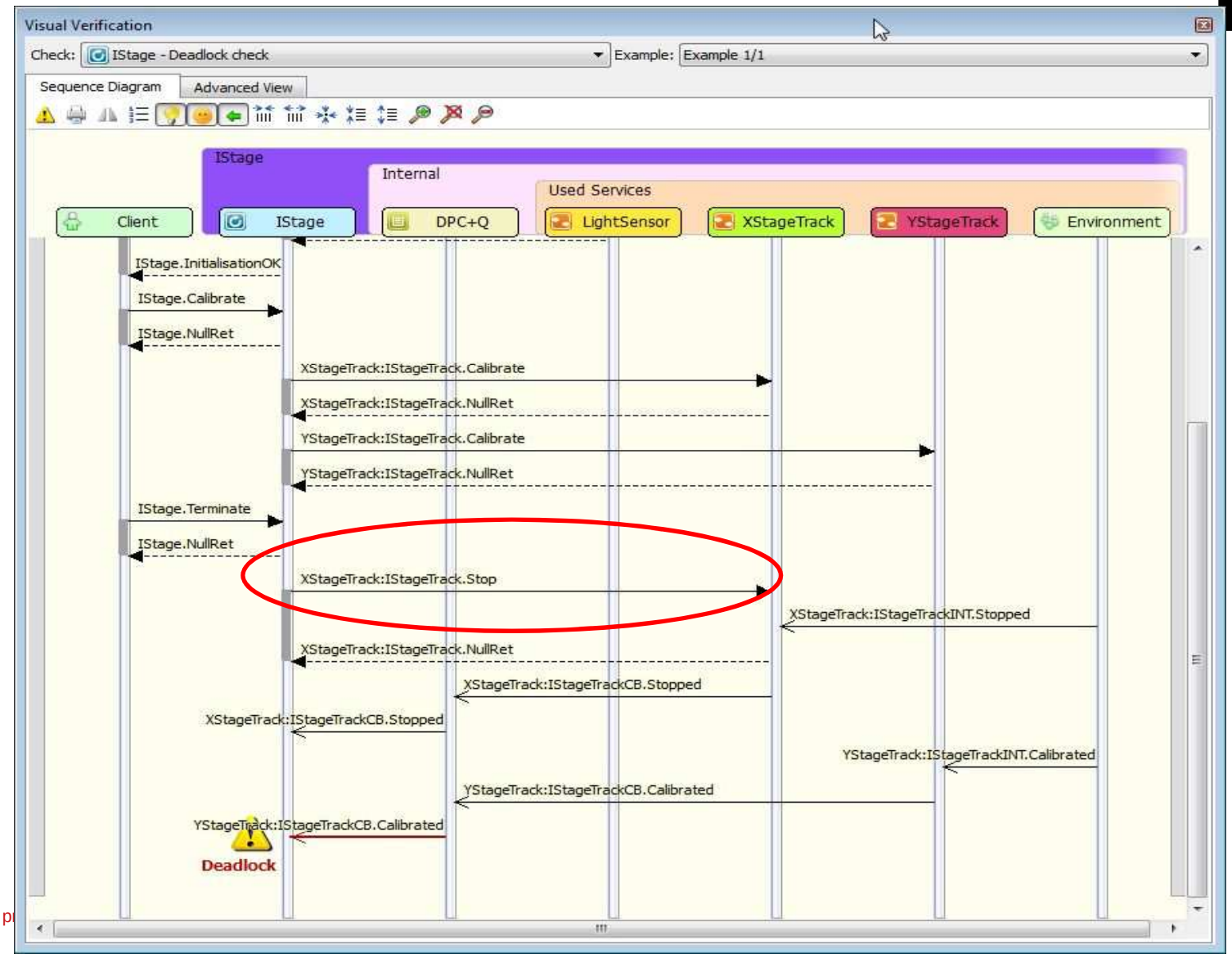
First attempt: results verification

verum



First attempt: results verification

verum



First attempt: change design model

verum

dm:IStage - ASD:Suite Release 3 - [IStage (Stage.dm)]

File Edit View Filters Tools Help

Stage | Used Services | Tags

SBS | States | State Variables

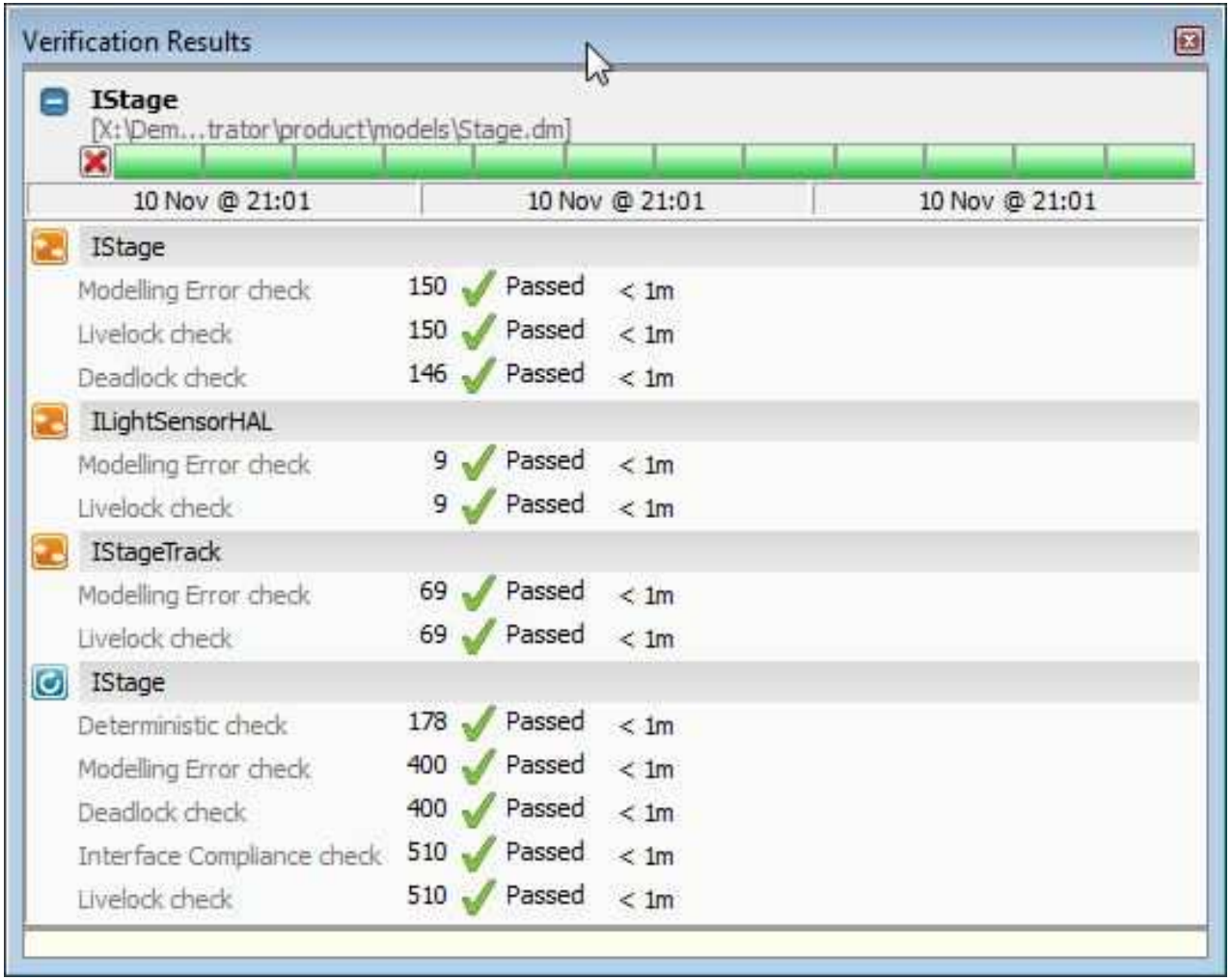
IStage.VoidReply; XStageTrack:IStageTrack.Stop

	Interface	Event	Guard	Actions	State Variable Updates	Target State	Comments	Tags
48	YStageTrack:IStageTrackCB	Terminated		Illegal		-	Misbehaving stage HAL - cannot occur b	
49	**Calibrating <IStage.Initialise+, IStage.Calibrate>**							
51	IStage	Initialise+		Illegal		-		
52	IStage	Terminate		IStage.VoidReply; XStageTrack:IStageTrack.Stop	XTrackStopped=false; YTrackStopped=false	Terminating_StoppingTracks	Demo: Induce dead-lock by removing one of the StageTrack.Stop responses.	
53	IStage	Start		Illegal		-		
54	IStage	LoadWafer		Illegal		-		
55	IStage	UnloadWafer		Illegal		-		
56	IStage	Stop		Illegal		-		
57	IStage	MoveToFOUPLoadPort		Illegal		-		
58	IStage	MoveToInputLoadPort		Illegal		-		
59	IStage	MoveToOutputLoadPort		Illegal		-		
60	IStage	MoveToInspectionUnit		Illegal		-		
61	IStage	Calibrate		Illegal		-		
65	XStageTrack:IStageTrackCB	Calibrated	YTrackHomed==false	NoOp	XTrackHomed=true	Calibrating	Was null	
66	XStageTrack:IStageTrackCB	Calibrated	YTrackHomed==true	IStageCB.CalibratedOK	XTrackHomed=true; StageAtUnload=false; StageAtInput=false; StageAtInspection=false; WaferLoaded=false	Calibrated		
67	XStageTrack:IStageTrackCB	Arrived		Illegal		-		
68	XStageTrack:IStageTrackCB	Stopped		Illegal		-		
69	XStageTrack:IStageTrackCB	Terminated		Illegal		-		
70	YStageTrack:IStageTrackCB	Calibrated	XTrackHomed==false	NoOp	YTrackHomed=true	Calibrating		
71	YStageTrack:IStageTrackCB	Calibrated	XTrackHomed==true	IStageCB.CalibratedOK	YTrackHomed=true; StageAtUnload=false; StageAtInput=false; StageAtInspection=false; WaferLoaded=false	Calibrated		
72	YStageTrack:IStageTrackCB	Arrived		Illegal		-		
73	YStageTrack:IStageTrackCB	Stopped		Illegal		-		
74	YStageTrack:IStageTrackCB	Terminated		Illegal		-		
75	**Terminating_StoppingTracks <IStage.Initialise+, IStage.Calibrate, IStage.Terminate>**							
77	IStage	Initialise+		Illegal		-		

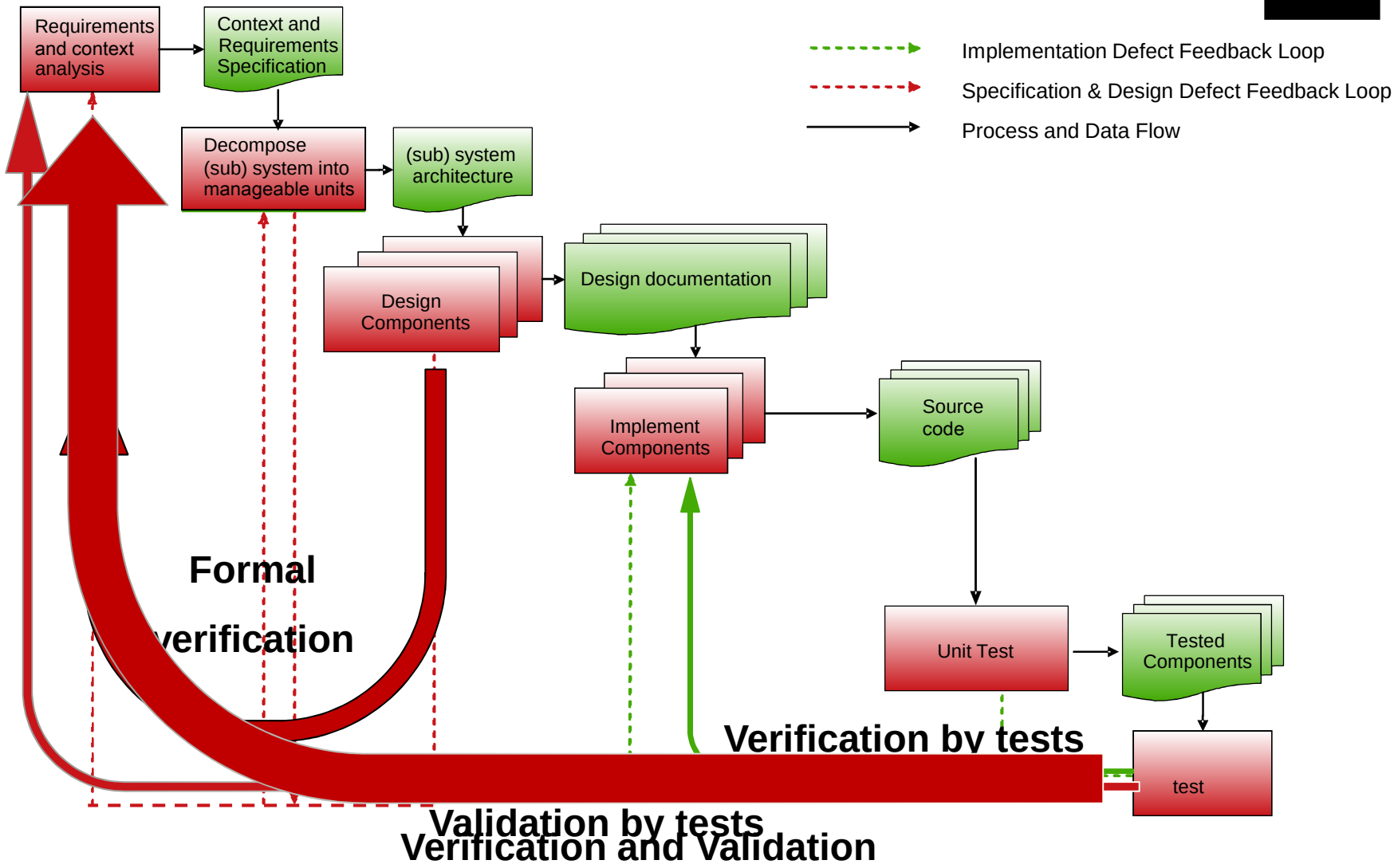
Model size: 625 ASD Function Points | C++ (7.0.0) | Connected

Second attempt: results verification

verum



Impact on development process

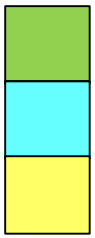


Impact on development process

verum

Cumulative effort in conventional software development

Cumulative effort based on ASD



Engineering: Requirements, Architecture, and Design

Implementation

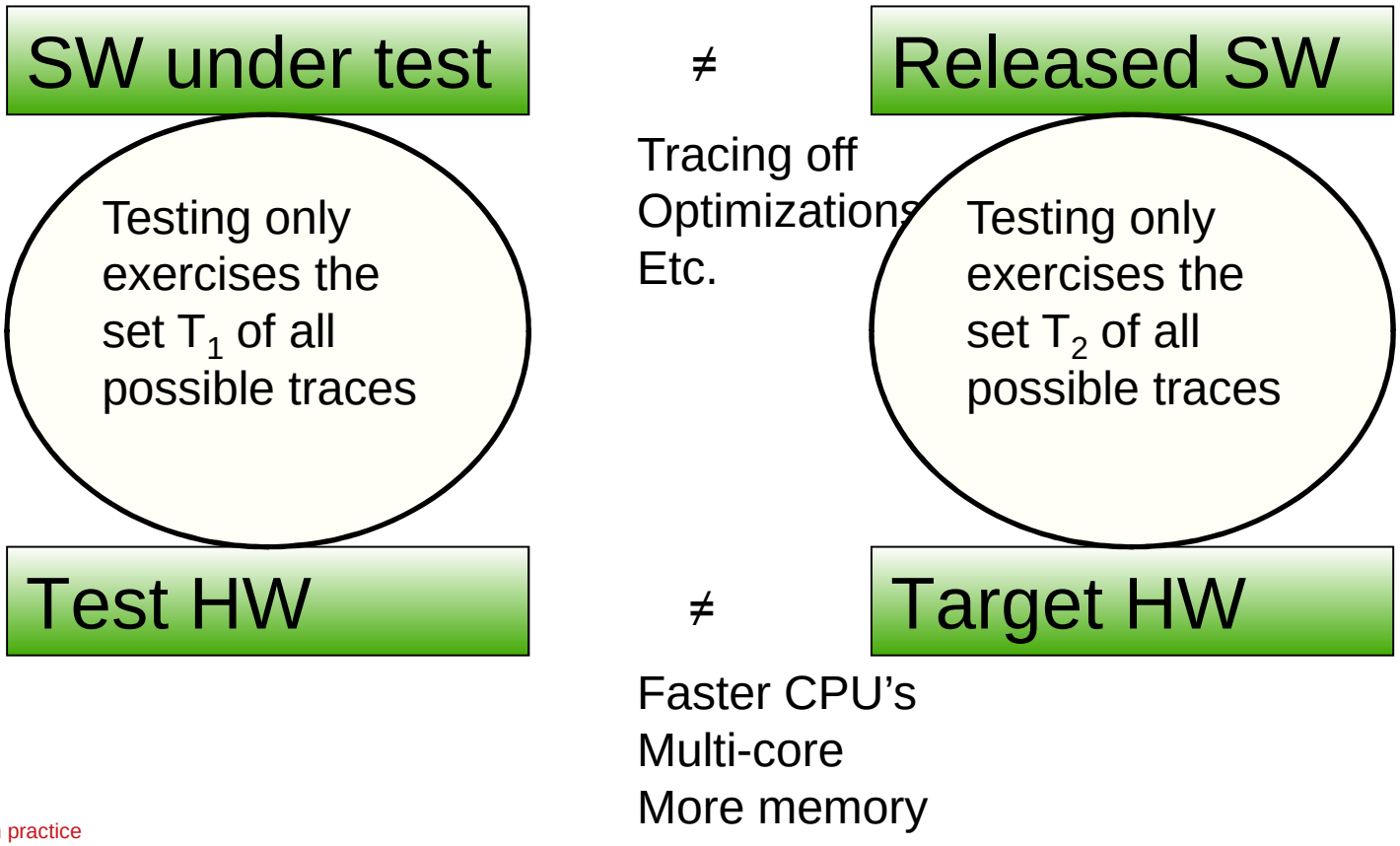
Integration & Testing

Practical difference between testing and verification

verum

Testing: finding (some, but not all) errors in $T_1 \cap T_2$

Verification: finding *all* errors in T_1 U T_2 U Untested traces



Impact on testing phase

verum

- Testing phase shorter:
  - Reduces to between 10-20% of end-to-end development work
- *Determine* quality rather than *establish* it
  - Increases objectivity of decision of release
  - Increases overall predictability of release
- Focus shifts from *verification* to *validation*
  - Test engineers must possess (more) domain knowledge

Future extensions ASD

verum

Lots, but the following ones impact (system) testing:

- More verification tests
  - E.g.: Check use of context parameters: write/initialize before read
- Component *validation* tests
  - Does component include certain behaviour
  - Does component exclude certain behaviour
- Long(er) term: design time simulation
  - Exploration design space supported by design time verification and validation
  - Focus from Testing towards Quality Assurance (like other sister-engineering disciplines)

And the results for the industry case?

verum

Nanda Tech

- 17 ASD components plus hand written software
- More than 100.000 execution scenarios verified
- 25.000 LOC in generated C# code
- Defect free software of ASD components in production use for several years now without one single reported (SW) failure!!

Ericsson Says…

verum

production & maintenance cost 30 to 50% down.

› First project: 350% productivity improvement.
20% lower cost results than available estimate.
1 month ahead of schedule.
Customer: T-Mobile Macedonia.

› Second project: 435% productivity improvement.
Customer: H3G Italy.

› Scale now

Questions